553, 984

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年9 月1 日 (01.09.2005)

PCT

(10) 国際公開番号
WO 2005/081450 A1

(51) 国際特許分類[7]: H04L 9/08, 9/32

(21) 国際出願番号: PCT/JP2004/019713

(22) 国際出願日: 2004 年12 月22 日 (22.12.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-48457 2004 年2 月24 日 (24.02.2004) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川 6 丁目 7 番 3 5 号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 佐藤 英雄 (SATO,Hideo) [JP/JP]; 〒141-0001 東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).

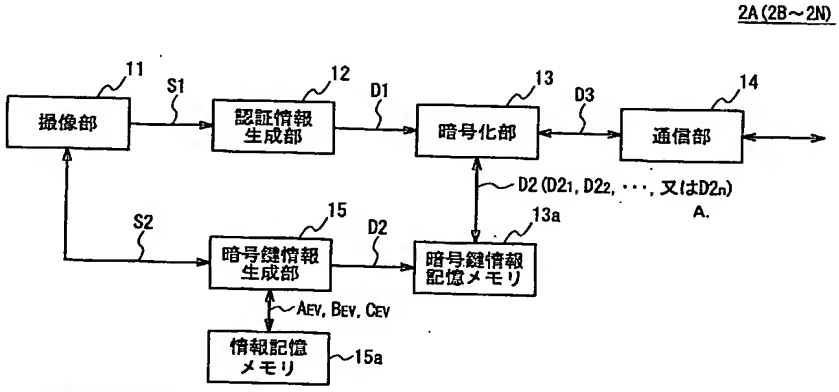
(74) 代理人: 田辺 恵基 (TANABE,Shigemoto); 〒141-0032 東京都 品川区 大崎 3 丁目 6 番 4 号 トキワビル 5 階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[続葉有]

(54) Title: ENCRYPTING APPARATUS AND ENCRYPTING METHOD

(54) 発明の名称: 暗号化装置及び暗号化方法



11.. IMAGING PART
12.. AUTHENTICATION INFORMATION PRODUCING PART
13.. ENCRYPTION PART
14.. COMMUNICATION PART
A.. D2 ($D2_1$, $D2_2$, ..., OR $D2_n$)
15.. ENCRYPTION KEY INFORMATION PRODUCING PART
15a.. INFORMATION STORAGE MEMORY
13a.. ENCRYPTION KEY INFORMATION STORAGE MEMORY

(57) Abstract: An encrypting apparatus and an encrypting method wherein the reliability of an encrypting function can be improved. A parameter specific to a solid-state imaging element is produced based on a uniform image signal (S2) outputted, from the solid-state imaging element, as an imaging result of a uniform subject in an imaging part (11). Encryption key information (D2) derived from the foregoing specific parameter is used to encrypt authentication information (D1). In this way, the concealment of the authentication information (D1) can be easily and simply maintained, so that the reliability of the encryption function can be improved.

(57) 要約: 暗号機能の信頼性を向上し得る暗号化装置及び暗号化方法を提案する。撮像部11における均一な撮像対象の撮像結果として固体撮像素子から出力される均一画像信号S2に基づいて当該固体撮像素子固有の素子

[続葉有]

WO 2005/081450 A1

SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

固有パラメータを生成し、この素子固有パラメータから導出した暗号鍵情報D2を用いて認証情報D1を暗号化するようにしたことにより、認証情報D1の秘匿性を簡易に確保することができ、かくして暗号機能の信頼性を向上することができる。

明　細　書

暗号化装置及び暗号化方法

技術分野

本発明は、暗号化装置及び暗号化方法に関し、例えば識別対象の正当性を証明するための情報（以下、これを認証情報と呼ぶ）を暗号化する場合に適用して好適なものである。

背景技術

従来、秘密鍵暗号方式又は公開鍵暗号方式に準拠した暗号化装置は、認証情報に対して、内部の不揮発性メモリに記憶された暗号鍵情報を用いて所定の暗号化処理を施すことにより暗号認証情報を生成し、これを復号化装置に送信するようになされている。

この場合、暗号化装置は、不揮発性メモリに記憶された暗号鍵情報の盗用をも防止して暗号機能の信頼性を確保するようになされており、当該暗号鍵情報の盗用を防止する手法として、暗号化装置内の深層部における所定の部材間に不揮発性メモリを搭載する手法、あるいは、不揮発性メモリと、当該不揮発性メモリに暗号鍵情報を記憶しておくときだけ暗号化する暗号復号化部を１つのチップとして搭載する手法（例えば特許文献１参照）がある。

特許文献１　特開２００３－２５６２８２公報。

ところでかかる暗号化装置においては、不揮発性メモリを搭載する際に煩雑化するのみならず、当該不揮発性メモリを搭載するものによる暗号鍵情報の盗用を避け得ず、この結果、暗号機能の信頼性を得るには未だ不十分であった。

発明の開示

本発明は以上の点を考慮してなされたもので、暗号機能の信頼性を向上し得る暗号化装置及び暗号化方法を提案しようとするものである。

かかる課題を解決するため本発明においては、秘匿対象の情報を暗号化する暗号化装置において、内部に有する複数の素子を単位とする素子群から出力される信号に基づいて、当該素子群における固有パラメータを生成する生成手段と、この生成手段により生成された固有パラメータを用いて情報を暗号化する暗号化手段とを設けるようにした。

また本発明においては、秘匿対象の情報を暗号化する暗号化方法において、内部に有する複数の素子を単位とする素子群から出力される信号に基づいて、当該素子群における固有パラメータを生成する第１のステップと、生成した固有パラメータを用いて情報を暗号化する第２のステップとを設けるようにした。

以上のように本発明によれば、内部に有する素子群における固有パラメータを用いて情報を暗号化するようにしたことにより、不揮発性メモリ等に予め保持させなくとも製造時であっても第三者には知り得ない固有パラメータを用いて暗号化することができるため、当該認証情報Ｄ１の秘匿性を簡易に確保することができ、かくして暗号機能の信頼性を向上することができる。

図面の簡単な説明

図１は、認証システムの構成を示すブロック図である。

図２は、本実施の形態による暗号化装置の構成を示すブロック図である。

図３は、撮像部の構成を示す略線図である。

図４は、復号化装置の構成を示すブロック図である。

発明を実施するための最良の形態

以下図面について本発明の一実施の形態を詳述する。

（１）認証システムの構成

図１において、１は全体として本実施の形態による認証システムの構成を示し、通信元の複数の暗号化装置２（２Ａ～２Ｎ）と、その通信相手の復号化装置３とが無線により接続されることにより構成されており、当該暗号化装置２と復号化装置３とが相互に各種情報を送受信することができるようになされている。

この場合、暗号化装置２は、復号化装置３との通信時にこの暗号化装置２を使用する使用者の所定部位における特徴パターンを認証情報として生成する。そして暗号化装置２は、この認証情報に対して所定の暗号化処理を施すことにより暗号認証情報を生成し、これを復号化装置３に送信するようになされている。

一方、復号化装置３は、このとき受信した暗号認証情報に対して所定の復号化処理を施すことにより認証情報を復元し、この認証情報を予め登録された対応する登録情報と照合する。

そして復号化装置３は、この照合結果に基づいて、このとき認証情報を送信した暗号化装置２を使用する使用者が正規の登録者であると判断した場合にのみ引き続き暗号化装置２との情報の授受を行うようになされている。

このようにしてこの認証システム１は、暗号化装置２を使用する使用者の正当性を、当該使用者自身の生体情報を用いて判断するようになされている。

（２）暗号化装置の構成

暗号化装置２（２Ａ～２Ｎ）は、それぞれ同一の構成であることによりここでは暗号化装置２Ａの構成について説明する。

この暗号化装置２Ａは、図２に示すように、指内方の血管を撮像対象として撮像する撮像部１１と、当該撮像部１１の撮像結果に基づいて認証情報を生成する認証情報生成部１２と、当該認証情報を暗号化する暗号化部１３と、所定の無線通信方式に準拠した通信処理を実行して情報の送受信を行う通信部１４とによって構成される。

この撮像部１１は、撮像部１１は、血管内の脱酸素化ヘモグロビン（静脈血）又は酸素化ヘモグロビン（動脈血）に近赤外線帯域の光（近赤外光）が特異的に吸収されることを利用して、当該血管を撮像するようになされている。

実際上、撮像部１１は、図３に示すように、近赤外光を発射する１又は２以上の光源２１を有し（図３では３つの光源を例として図示している）、光源２１から発射される近赤外光の光路上には、当該近赤外光のうち特定の近赤外線帯域の光を透過する第１のフィルタ２２、当該第１のフィルタ２２を介して得られる光のうち静脈血に吸収される近赤外線帯域とその付近との光を透過する第２のフィルタ２３及び固体撮像素子２４が順次配置される。

またこの撮像部１１には、近赤外光の光路上以外の位置（以下、これを光路外位置と呼ぶ）Ｐ１に散光板２５が設けられており、この散光板２５は、光路外位置Ｐ１と、固体撮像素子２４から所定距離を隔てた前面の位置（以下、これを光路上位置と呼ぶ）Ｐ２との間を移動自在となっている。

そしてこの撮像部１１においては、第１のフィルタ２２と第２のフィルタ２３との間に指ＦＧを介挿することができるようになされていると共に、当該指ＦＧの介挿時に近赤外光の光路に対する雰囲気中の外光の入射を遮蔽する遮蔽部２６が設けられており、これにより指ＦＧ内方における血管の撮像時に遮蔽部２６外における可視光や紫外光による近赤外光への影響を低減することができるようになされている。

この場合、撮像部１１は、第１及び第２のフィルタ２２、２３間に指ＦＧが介挿された状態において撮像命令コマンドが与えられると、光源２１から近赤外光を発射し、これを第１のフィルタ２２を介して指ＦＧに照射する。

この近赤外光は指ＦＧ内方における血管組織では内在するヘモグロビンに特異的に吸収されるため、当該指ＦＧを経由して得られる近赤外光は血管組織の形成パターンを表す血管パターン光として、第２のフィルタ２３を介して固体撮像素子２４に入射することとなる。

そして撮像部１１は、かかる血管パターン光を固体撮像素子２４に配された複数の光電変換素子により光電変換し、これら光電変換素子において生成された血管画像信号Ｓ１を認証情報生成部１２（図２）に送出する。

このようにして撮像部１１は、生体内方に有する血管を撮像対象として撮像す

ることができるようになされている。

認証情報生成部１２は、供給される血管画像信号Ｓ１に対してＡ／Ｄ（Ａｎ－ａｌｏｇ／Ｄｉｇｉｔａｌ）変換処理を施すことにより血管画像データを生成し、この血管画像データに基づく血管画像のうち、予め指定された領域に有する血管を抽出する。そして認証情報生成部１２は、抽出した血管の形成パターンを認証情報Ｄ１として生成し、これを暗号化部１３に送出する。

暗号化部１３は、所定のアルゴリズムにより順次生成された複数の暗号鍵情報を記憶するメモリ（以下、これを暗号鍵情報記憶メモリと呼ぶ）１３ａを有しており、当該暗号鍵情報記憶メモリ１３ａに記憶された複数の暗号鍵情報Ｄ２（$D2_1$～$D2_n$）のうち、通信部１４を介して復号化装置３（図１）からの指定要求に対応する例えば暗号鍵情報$D2_1$を選択し、これを読み出す。

そして暗号化部１３は、供給される認証情報Ｄ１に対して、このとき読み出した暗号鍵情報$D2_1$を用いて例えばＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）　に準拠した暗号化処理を施すことにより暗号認証情報Ｄ３を生成し、これを通信部１４を介して復号化装置３（図１）に送信するようになされている。

このように暗号化装置２Ａは、生体内方に有する固有の血管形成パターンを認証情報Ｄ１として生成することにより、当該生体表面に有する指紋等を認証情報として生成する場合に比して生体からの直接的な盗用を防止できるため、暗号化装置２Ａを使用する使用者が登録者になりすますといった事態を未然に回避することができるようになされている。

（３）暗号鍵情報生成処理

かかる構成に加えて、この暗号化装置２Ａは、撮像部１１における均一な撮像対象の撮像結果に基づいて、この暗号化装置２Ａ固有の複数の暗号鍵情報Ｄ２（$D2_1$～$D2_n$）を生成するようになされている。

この場合、暗号化装置２Ａは、復号化装置３（図１）から通信部１４を介して暗号鍵情報の生成要求を受けるごとに所定の暗号鍵情報生成処理をその都度実行

し、この結果得られた暗号鍵情報Ｄ２を暗号化部１３の暗号鍵情報記憶メモリ１３ａに記憶又は更新するようになされている。以下、この暗号鍵情報生成処理を実行する暗号鍵情報生成部１５について説明する。

この暗号鍵情報生成部１５は、復号化装置３からの生成要求があった場合に、撮像部１１に対して均一な撮像対象を撮像させ、当該撮像した結果得られる信号に基づいて暗号鍵情報を生成するようになされている。

実際上、暗号鍵情報生成部１５は、撮像部１１（図３）の散光板２５が光路外位置Ｐ１から光路上位置Ｐ２に配置されるように制御すると共に、撮像部１１に撮像命令コマンドを送出する。

この場合、撮像部１１（図３）では、光源２１から発射された近赤外光は、第１及び第２のフィルタ２２、２３を順次介して散光板２５に照射され、当該散光板２５において固体撮像素子２４に対して均一な拡散光（以下、これを均一拡散光と呼ぶ）として拡散されて、固体撮像素子２４に入射することとなる。

ここで、この固体撮像素子２４には、当該固体撮像素子２４に格子状に配された複数の光電変換素子に対応させて開口部及び集光レンズがそれぞれ設けられているが、これら開口部及び集光レンズの形状には製造工程上の様々な要因によってばらつきがあり、このばらつきが固体撮像素子２４固有となっている。

従って、固体撮像素子２４での均一拡散光に対する光電変換結果として暗号鍵情報生成部１５（図２）に入力される信号（以下、これを均一画像信号と呼ぶ）Ｓ２には、製造時には知り得ない固体撮像素子２４固有のばらつきがノイズパターン（以下、これをばらつきパターンと呼ぶ）として含まれることとなる。

そして暗号鍵情報生成部１５は、このようにして得られた均一画像信号Ｓ２に対してＡ／Ｄ変換処理を施すことにより均一画像データを生成し、この均一画像データに基づいて固体撮像素子２４における固有のばらつきパターンに起因するパラメータ（以下、これを素子固有パラメータと呼ぶ）を生成する。

この実施の形態の場合、暗号鍵情報生成部１５では、かかる素子固有パラメータを生成する手法として、均一画像データに対する所定の評価パターンと均一画

像データとのハミング距離を算出し、当該算出結果を素子固有パラメータとして生成する手法が採用されている。

具体的に暗号鍵情報生成部１５は、互いにハミング距離の離れた例えば３つのデータ列が評価パターンA_{EV}、B_{EV}、C_{EV}として記憶された情報記憶メモリ１５ａを有しており、これら評価パターンA_{EV}、B_{EV}、C_{EV}用いて、均一画像データのうち評価パターンと同一データ長となる上位の均一画像データ（以下、これを上位均一画像データと呼ぶ）を「Ｘ」とし、排他的論理和（ＸＯＲ）を「^」とすると、次式

$$dH(x, A_{EV}) = \Sigma xi \wedge Ai = Xa$$

$$dH(x, B_{EV}) = \Sigma xi \wedge Bi = Xb \quad \cdots\cdots (1)$$

$$dH(x, C_{EV}) = \Sigma xi \wedge Ci = Xc$$

但し、$i = 1 \sim n$

に従って、上位均一画像データＸと、評価パターンA_{EV}、B_{EV}、C_{EV}それぞれとのハミング距離Ｘａ、Ｘｂ、Ｘｃをそれぞれ算出し、これらハミング距離Ｘａ、Ｘｂ、Ｘｃを所定の順序で組み合わせ、当該組み合わせを素子固有パラメータとして生成するようになされている。

この場合、暗号鍵情報生成部１５は、上位均一画像データＸと各評価パターンA_{EV}、B_{EV}、C_{EV}との相関結果を素子固有パラメータとして生成するため、撮像時の撮像状態に応じて均一画像データが変化した場合であっても、ばらつきパターンに起因する素子固有パラメータの再現性を維持することができるようになされている。

またこの場合、暗号鍵情報生成部１５は、製造後の固体撮像素子２４から出力される均一画像信号Ｓ２に基づいて素子固有パラメータを生成するため、当該固体撮像素子２４の製造者に対して知り得ない情報として生成することができるの

みならず、当該固体撮像素子２４のばらつきパターン自体ではなく各評価パターンA_{EV}、B_{EV}、C_{EV}との相関結果の組み合わせを素子固有パラメータとして生成するため、この暗号化装置２の製造者や固体撮像素子２４を盗用したものに対しても知り得ない情報として生成することができるようになされている。

次いで暗号鍵情報生成部１５は、このようにして生成した素子固有パラメータをシードとして所定のアルゴリズムにより複数の暗号鍵情報Ｄ２（$D2_1$～$D2_n$）を生成し、当該暗号鍵情報Ｄ２を暗号化部１３の暗号鍵情報記憶メモリ１３ａに記憶又は更新するようになされている。

この結果、暗号化部１３に供給される認証情報Ｄ１は、この暗号化装置（固体撮像素子２４）固有の例えば暗号鍵情報$D2_1$を用いた暗号化処理により暗号認証情報Ｄ３として生成され、通信部１４を介して復号化装置３に送信されることとなる。

なお、暗号鍵情報生成部１５は、新たに複数の暗号鍵情報Ｄ２を生成した場合には、所定の登録処理により又は暗号鍵情報Ｄ２に対して所定の暗号化処理を施した後に復号化装置３に送信することにより、当該新たに生成した複数の暗号鍵情報Ｄ２を復号化装置３のデータベースに登録しておくようになされている。

このようにこの暗号化装置２は、製造時には知り得ない素子固有パラメータから導出した暗号鍵情報Ｄ２を用いて認証情報Ｄ１を暗号化することにより、暗号化装置２を使用する使用者の登録者へのなりすましをより回避して暗号機能の信頼性を格段に高めることができるようになされている。

（４）復号化装置の構成

復号化装置３は、図４に示すように、所定の無線通信方式に準拠した通信処理を実行して情報の送受信を行う通信部３０と、暗号化装置２（２Ａ～２Ｎ）に対して各種要求を行う要求部３１と、当該通信部３０で受信された結果得られる暗号認証情報Ｄ３を復号化する復号化部３２と、当該復号化部３２での復号結果を用いて所定の認証処理を実行する照合部３３と、登録データベースＤＢとによって構成される。

この登録データベースＤＢには、所定の登録処理により、暗号化装置２（２Ａ～２Ｎ）の撮像部１１で撮像される血管と同一部位における血管の形成パターンと、当該暗号化装置２（２Ａ～２Ｎ）の固体撮像素子２４における同一の素子固有パラメータから導出された複数の暗号鍵情報Ｄ２とがそれぞれ登録情報Ｄ１０（$D10_1$～$D10_n$）として登録されている。

この場合、要求部３１は、通信部３０を介して接続した暗号化装置２（２Ａ～２Ｎ）に対して、所定のタイミングで認証処理時における各種条件を要求するようになされており、当該条件として複数の暗号鍵情報のうち、使用する暗号鍵情報$D2_1$、$D2_2$、……、又は$D2_n$の番号やその他の事項を要求する。この場合、要求部３１は、指定した暗号鍵情報の番号を復号化部３２に通知するようになされている。

また要求部３１は、必要に応じて暗号鍵情報Ｄ２の生成を要求するようになされており、この場合、登録データベースＤＢに登録された対応する登録情報$D10_1$、$D10_2$、……、又は$D10_n$の暗号鍵情報Ｄ２を、所定の登録処理又は通信部３０を介して得られる暗号化装置２によって新たに生成された暗号鍵情報に更新するようになされている。

復号化部３２は、通信部３０を介して供給される暗号認証情報Ｄ３のヘッダに記述される送信元アドレス基づいて、登録データベースＤＢのなかから例えば暗号化装置２Ａに対応する登録情報$D10_1$を読み出し、当該登録情報$D10_1$の複数の暗号鍵情報$D2_1$～$D2_n$のうちこのとき要求部３１から通知された暗号化情報$D2_1$を選択する。

そして復号化部３２は、暗号認証情報Ｄ３に対して、このとき選択した暗号鍵情報$D2_1$を用いて暗号化装置２Ａと同一の暗号化処理を施すことにより認証情報Ｄ１を復元し、当該認証情報Ｄ１及び対応する登録情報$D10_1$を照合部３３に送出する。

照合部３３は、供給される認証情報Ｄ１の血管形成パターンと、対応する登録情報$D10_1$の血管形成パターンとを所定の手法により照合するようになされて

おり、この照合結果として所定の合致率が得られなかった場合には、このとき認証情報Ｄ１を送信した暗号化装置２Ａを使用する使用者が不正使用する第三者であると判断し、その後の暗号化装置２Ａとの情報の授受を停止するように通信部３０を制御する。

これに対して照合部３３は、所定の合致率が得られた場合には、このとき認証情報Ｄ１を送信した暗号化装置２Ａを使用する使用者が正規の使用者であると判断し、この場合には暗号化装置２Ａと、内部に設けられた情報処理部（図示せず）との間で情報の授受を行うように通信部３０を制御するようになされている。

このようにして復号化装置３は、生体固有の認証情報Ｄ１（血管形成パターン）と、固体撮像素子２４固有の固有素子パラメータから導出された暗号鍵情報Ｄ２とを用いて認証処理を実行することができるようになされている。

（５）本実施の形態による動作及び効果

以上の構成において、この暗号化装置２（２Ａ～２Ｎ）は、撮像部１１における均一な撮像対象の撮像結果として固体撮像素子２４から出力される均一画像信号Ｓ２に基づいて、当該固体撮像素子２４固有の素子固有パラメータを生成する。

そして暗号化装置２（２Ａ～２Ｎ）は、この素子固有パラメータから導出した所定の暗号鍵情報Ｄ２を用いて認証情報Ｄ１を暗号化する。

従って暗号化装置２（２Ａ～２Ｎ）は、従来のように不揮発性メモリ等に予め暗号化鍵を保持させなくとも、製造時であっても第三者には知り得ない素子固有パラメータから導出した暗号鍵情報Ｄ２を生成することができるため、当該認証情報Ｄ１の秘匿性を簡易に確保することができる。

以上の構成によれば、均一な撮像対象の撮像結果として固体撮像素子２４から出力される均一画像信号Ｓ２に基づいて当該固体撮像素子２４固有の素子固有パラメータを生成し、この素子固有パラメータから導出した所定の暗号鍵情報Ｄ２を用いて認証情報Ｄ１を暗号化するようにしたことにより、認証情報Ｄ１の秘匿性を簡易に確保することができ、かくして暗号機能の信頼性を向上することがで

きる。

（６）他の実施の形態

なお上述の実施の形態においては、内部に有する複数の素子を単位とする素子群から出力される信号に基づいて、素子群における固有パラメータを生成する生成手段として、固体撮像素子２４に配された複数の光電変換素子から出力される均一画像信号Ｓ２に基づいて、当該固体撮像素子２４における固有の素子固有パラメータを生成するようにした場合について述べたが、本発明はこれに限らず、例えばタッチパッドの圧電素子群から出力される信号に基づいて固有パラメータを生成するようにしても良く、この他種々の能動素子や受動素子の集合を単位とする素子群における固有パラメータを生成することができる。

この場合、素子群は、単一種類であっても複数種類であっても上述の実施の形態と同様の効果を得ることができる。

また固有パラメータの生成手法として、素子群から出力される均一画像信号Ｓ２のデータを、直接、記憶手段としての情報記憶メモリに記憶された互いに異なる３つの評価パターンA_{EV}、B_{EV}、C_{EV}との間におけるハミング距離（相関値）を算出し、これら算出結果を所定順序で組み合わせるようにした場合について述べたが、本発明はこれに限らず、均一画像信号Ｓ２のデータに対してＦＦＴ（Ｆａｓｔ　Ｆｏｕｒｉｅｒ　Ｔｒａｎｓｆｏｒｍ）処理を施し、この処理結果と評価パターンA_{EV}、B_{EV}、C_{EV}とのハミング距離の算出結果を組み合わせるようにしても良く、あるいはＦＦＴ処理結果のうち低周波成分のデータのみに対して逆ＦＦＴ処理施し、この処理結果と評価パターンA_{EV}、B_{EV}、C_{EV}とのハミング距離の算出結果を組み合わせるようにしても良く、又はこれら処理結果を組み合わせるようにしても良い。このようにすれば、より秘匿性の高くかつ再現性の優れた固有パラメータを生成することができるため、暗号機能の信頼性を格段に向上することができる。

この場合、撮像部１１に対して散光板２５を撮像させ、当該撮像結果として得られる信号に基づいて固有パラメータを暗号鍵情報として生成する暗号鍵情報生

成部１５を適用するようにしたが、本発明はこれに限らず、散光板２５以外の均一な撮像対象を撮像させるようにしても良く、また暗号鍵情報を生成せずに固有パラメータのみを生成するようにしても良く、要は、固有パラメータを生成するこの他種々の生成部を適用することができる。

またこの場合、生成時期として、復号化装置３から通信部１４を介して暗号鍵情報の生成要求を受けることに生成するようにした場合について述べたが、本発明はこれに限らず、製造時にのみ生成する等、この他種々のタイミングで生成することができる。

さらに評価パターンとして、所定の評価パターンを予め情報記憶メモリに記憶するようにしたが、本発明はこれに限らず、複数の評価パターンを情報記憶メモリに記憶しておき、この評価パターンのうちから予め規定された数の評価パターンを選択するようにしても良く、またこのとき選択する評価パターンを復号化装置３の要求に応じて変更するようにしても良く、あるいは所定タイミング時に所定のアルゴリズムにより生成した評価パターンを情報記憶メモリに記憶するようにしても良い。このようにすれば、仮に、認証情報Ｄ１が盗用された場合及び暗号鍵情報から評価パターンが解読された場合であっても、対応する評価パターンを用いないようにすることができるため、暗号機能の信頼性を格段に向上することができる。

さらに評価パターンの数として、３種類の評価パターンを情報記憶メモリに記憶するようにしたが、本発明はこれに限らず、少なくとも２以上の評価パターンを情報記憶メモリに記憶していれば、上述の実施の形態と同様の効果を得ることができる。

また上述の実施の形態においては、固有パラメータを用いて情報を暗号化する暗号化手段として、固有パラメータから導出した暗号鍵情報を用いて血管形成パターンからなる認証情報Ｄ１を暗号化する暗号化部１３を適用するようにした場合について述べたが、本発明はこれに限らず、固有パラメータにより認証情報Ｄ１を暗号化する暗号化部を適用するようにしても良い。

この場合、生体内方の血管形成パターンを認証情報Ｄ１として暗号化するようにしたが、本発明はこれに限らず、例えば指紋等の生体表面の特徴パターン等、この他種々の生体情報を認証情報として暗号化することができ、また認証情報や生体情報である必要はなく、要は、秘匿対象とすべき情報を暗号化すれば良い。

産業上の利用可能性

本発明は、パーソナルコンピュータや携帯電話機等の端末装置や、家庭用電子機器等の装置であって、外部の装置に対して自身を識別させる場合に利用可能である。

請 求 の 範 囲

1．秘匿対象の情報を暗号化する暗号化装置において、

内部に有する複数の素子を単位とする素子群から出力される信号に基づいて、上記素子群における固有パラメータを生成する生成手段と、

上記生成手段により生成された上記固有パラメータを用いて上記情報を暗号化する暗号化手段と

を具えることを特徴とする暗号化装置。

2．上記生成手段は、

互いに異なる複数の評価パターンを記憶する記憶手段を具え、

上記記憶手段に記憶された各上記評価パターンそれぞれに対する上記信号の相関値の組み合わせを上記固有パラメータとして生成する

ことを特徴とする請求の範囲第1項に記載の暗号化装置。

3．所定の通信相手と通信する通信手段を具え、

上記生成手段は、

上記通信相手から要求された各上記評価パターンを、上記記憶手段に記憶された各上記評価パターンのなかから選択し、当該選択した各上記評価パターンそれぞれに対する上記信号の相関値の組み合わせを上記固有パラメータとして生成する

ことを特徴とする請求の範囲第2項に記載の暗号化装置。

4．所定の撮像対象を撮像する固体撮像素子を具え、

上記生成手段は、

均一な上記撮像対象の撮像結果として上記固体撮像素子から出力される信号に基づいて、上記固体撮像素子における上記固有パラメータを生成する

ことを特徴とする請求の範囲第１項に記載の暗号化装置。

５．所定の撮像対象を撮像する固体撮像素子を具え、

上記生成手段は、

均一な上記撮像対象の撮像結果として上記固体撮像素子から出力される信号に基づいて、上記固体撮像素子における上記固有パラメータを生成するパラメータ生成手段と、

生体の表面又は上記生体の内方の撮像結果として上記固体撮像素子から出力される信号に基づいて、上記生体固有の生体情報を生成する生体情報生成手段とを具え、

上記暗号化手段は、

上記パラメータ生成手段により生成された上記固有パラメータを用いて、上記生体情報生成手段により生成された上記生体情報を暗号化する

ことを特徴とする請求の範囲第１項に記載の暗号化装置。

６．秘匿対象の情報を暗号化する暗号化方法において、

内部に有する複数の素子を単位とする素子群から出力される信号に基づいて、上記素子群における固有パラメータを生成する第１のステップと、

生成した上記固有パラメータを用いて上記情報を暗号化する第２のステップと

を具えることを特徴とする暗号化方法。

７．上記第１のステップでは、

互いに異なる複数の評価パターンそれぞれに対する上記信号の相関値の組み合わせを上記固有パラメータとして生成する

ことを特徴とする請求の範囲第６項に記載の暗号化方法。

８．上記第１のステップでは、

各上記評価パターンのなかから、所定の通信相手からの要求に対応する各上記評価パターンを選択し、当該選択した各上記評価パターンそれぞれに対する上記信号の相関値の組み合わせを上記固有パラメータとして生成する

ことを特徴とする請求の範囲第７項に記載の暗号化方法。

９．上記第１のステップでは、

均一な撮像対象の撮像結果として固体撮像素子から出力される信号に基づいて、上記固体撮像素子における上記固有パラメータを生成する

ことを特徴とする請求の範囲第６項に記載の暗号化方法。

１０．上記第１のステップでは、

均一な撮像対象の撮像結果として固体撮像素子から出力される信号に基づいて、上記固体撮像素子における上記固有パラメータを生成するパラメータ生成ステップと、

生体の表面又は上記生体の内方の撮像結果として上記固体撮像素子から出力される信号に基づいて、上記生体固有の生体情報を生成する生体情報生成ステップと

を具え、

上記第２のステップでは、

上記固有パラメータを用いて上記生体情報を暗号化する

ことを特徴とする請求の範囲第６項に記載の暗号化方法。

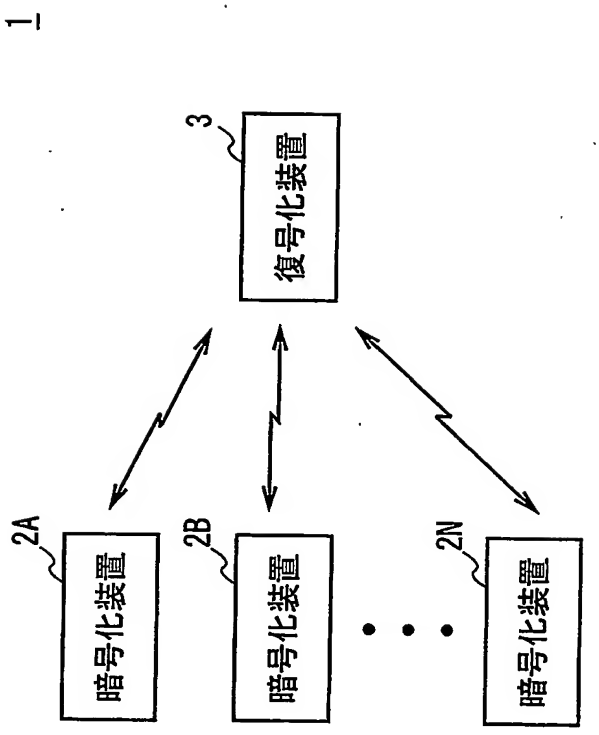


図 1

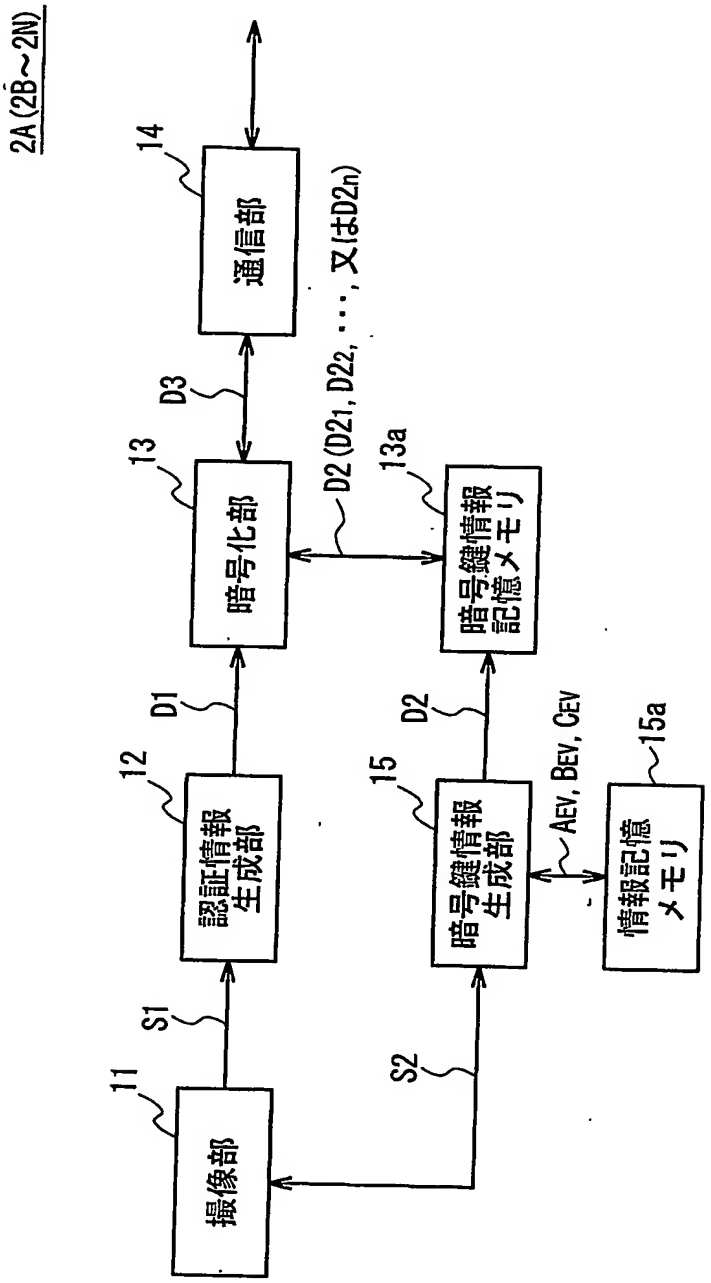

2A(2B~2N)
14
通信部
D3
13
暗号化部
D2 (D21, D22, ・・・, 又はD2n)
13a
暗号鍵情報記憶メモリ
D1
D2
12
認証情報生成部
15
暗号鍵情報生成部
AEV, BEV, CEV
15a
情報記憶メモリ
S1
S2
11
撮像部

図2

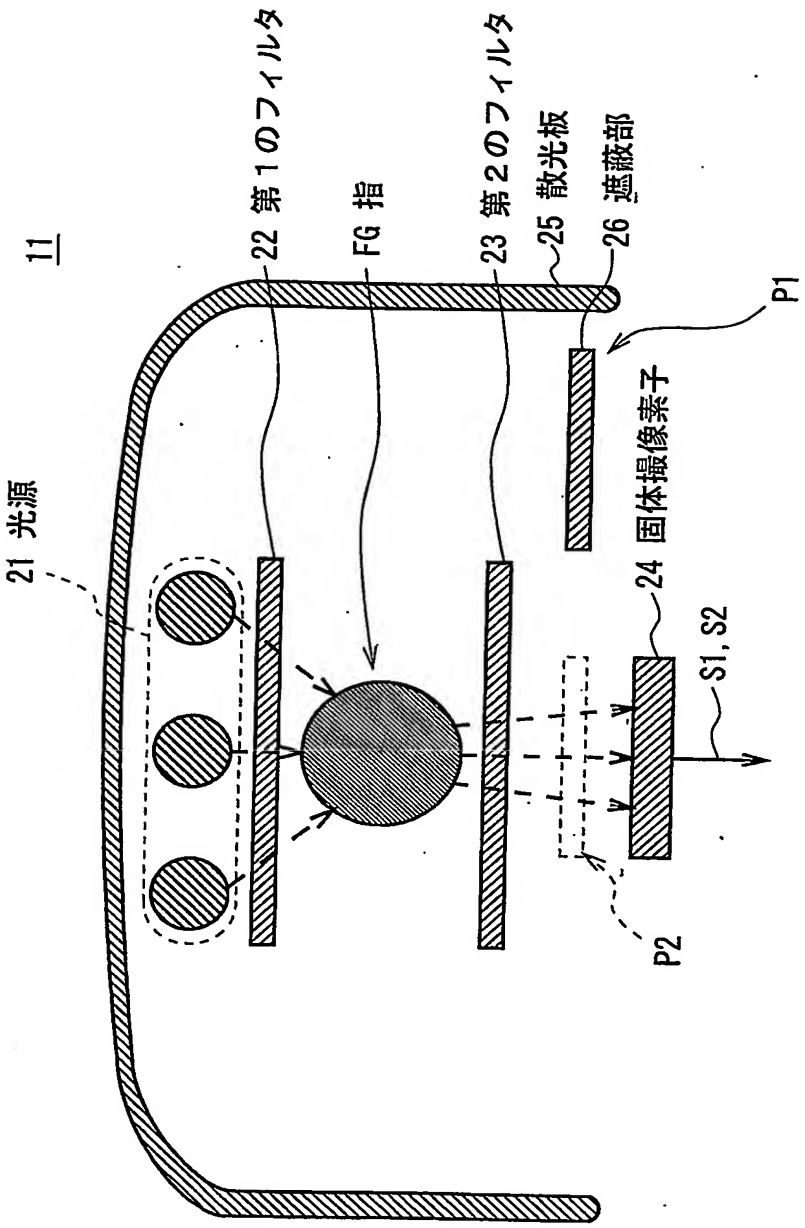

11
21 光源
22 第1のフィルタ
FG 指
23 第2のフィルタ
25 散光板
26 遮蔽部
P1
24 固体撮像素子
S1, S2
P2

図3

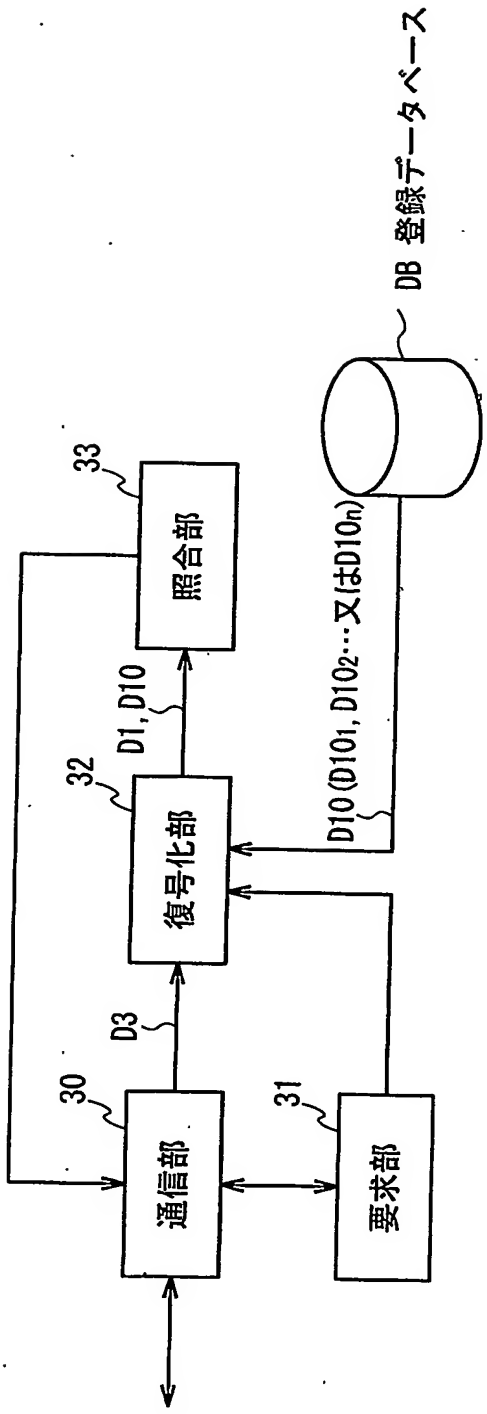

DB 登録データベース
D10(D10₁, D10₂…又はD10n)
33
照合部
D1, D10
32
復号化部
D3
30
通信部
31
要求部

図4

符 号 の 説 明

１……認証システム、２……暗号化装置、３……復号化装置、１１……撮像部、１２……認証情報生成部、１３……暗号化部、１３ａ……暗号鍵情報記憶メモリ、１５……暗号鍵情報生成部、１５ａ……情報記憶メモリ、２４……固体撮像素子

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/019713

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Jitsuyo Shinan Toroku Koho 1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2002-73424 A (Mitsubishi Electric Corp.), 12 March, 2002 (12.03.02), Par Nos. [0171] to [0176]; Figs. 26, 32 & US 2002/0024453 A1 & DE 10141438 A1 & KR 2002073424 A & TW 506067 A	1,6 2-5,7-10
Y A	JP 2003-248578 A (ST Microelectronics S.A.), 05 September, 2003 (05.09.03), Par Nos. [0001] to [0045]; Fig. 1 & US 2003/0103629 A1 & FR 2833119 A1 & EP 1359551 A1	1,6 2-5,7-10

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 February, 2005 (15.02.05)	01 March, 2005 (01.03.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号　PCT／JP2004／019713

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ H04L9／08, H04L9／32

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ H04L9／08, H04L9／32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2005年
日本国登録実用新案公報	1994－2005年
日本国実用新案登録公報	1996－2005年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2002-73424 A（三菱電機株式会社）2002.03.12, 段落【0171】－【0176】, 図26,32 & US 2002/0024453 A1	1,6
A	& DE 10141438 A1 & KR 2002073424 A & TW 506067 A	2-5,7-10
Y	JP 2003-248578 A（エステーミクロエレクトロニクス　ソシエテアノニム）2003.09.05,	1,6
A	段落【0001】－【0045】, 図1 & US 2003/0103629 A1 & FR 2833119 A1 & EP 1359551 A1	2-5,7-10

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日　15.02.2005	国際調査報告の発送日　01.3.2005
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里　裕正　5M　3365 電話番号　03－3581－1101　内線　3597